

Bipartite All-Versus-Nothing Proofs of Bell's Theorem with Single-Qubit Measurements

Adán Cabello* and Pilar Moreno

Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain

(Dated: February 1, 2008)

If n qubits were distributed between 2 parties, which quantum pure states and distributions of qubits would allow all-versus-nothing (or Greenberger-Horne-Zeilinger-like) proofs of Bell's theorem using only single-qubit measurements? We show a necessary and sufficient condition for the existence of these proofs for *any* number of qubits, and provide *all* distinct proofs up to $n = 7$ qubits. Remarkably, there is only one distribution of a state of $n = 4$ qubits, and six distributions, each for a different state of $n = 6$ qubits, which allow these proofs.

PACS numbers: 03.65.Ud, 03.65.Ta, 03.67.Mn, 42.50.Xa

The Greenberger-Horne-Zeilinger (GHZ) proof [1, 2] of Bell's theorem [3] not only “opened a new chapter on the hidden variables problem” [4] and made “the strongest case against local realism since Bell's work” [5]; it also inspired the quantum protocols for reducing communication complexity [6] and for secret sharing [7], and motivated the study of multipartite entanglement [8]. The GHZ proof provides a direct contradiction, using qubits and without requiring inequalities, between Einstein, Podolsky, and Rosen's (EPR's) criterion of elements of reality [9] and perfect correlations predicted by quantum mechanics. Mermin coined the name “all-versus-nothing” (AVN) for proofs like GHZ's, based on m perfect correlations such that, if we assume elements of reality, $m - 1$ of them lead us to the conclusion that it is the *opposite* of the one given by the m th correlation [10].

However, while the original proof of Bell's theorem required only 2 separated parties, the GHZ proof required 3 because, when the qubits are distributed between 2 parties, there is no physical reason supporting the assumption that all single-qubit observables appearing in the proof have predefined results, since some of them do *not* satisfy EPR's criterion of elements of reality. EPR's criterion states that: “if, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity” [9]. Applied to the bipartite case, this means that it must be possible to predict with certainty the results of measuring all observables appearing in the proof on Alice's (Bob's) side from the results of spacelike separated measurements on Bob's (Alice's) side.

The first 2-party AVN proof with qubits was introduced in [11, 12], then adapted for 2 photons [13], and finally tested in the laboratory [14, 15]. One of the difficulties of experimentally implementing this 2-party AVN proof was that it required 2-qubit local measurements [16]. The first 2-party AVN proof requiring only single-qubit measurements was introduced in [17, 18] and

has been recently demonstrated in the laboratory [19]. These bipartite AVN proofs required 4-qubit states with 2 qubits each on Alice's and Bob's sides.

The possibilities brought forth by recent developments like 2-photon hyperentangled states (i.e., entangled in several degrees of freedom) encoding 3 or more qubits in each photon [20], and 6-photon 6-qubit states [21, 22], naturally lead to the following problem: If n qubits were distributed between 2 parties, which are the quantum pure states and possible distributions of qubits that allow a 2-party AVN proof using only single-qubit measurements?

This problem is also related to the one of finding genuinely new bipartite communication complexity problems with a quantum advantage (specifically, new schemes of quantum pseudotelepathy [23]), and to the problem of deciding which n -qubit states and distributions of qubits allow bipartite EPR-Bell inequalities [24, 25].

In this Letter we show a necessary and sufficient condition for the existence of bipartite AVN proofs using only single-qubit measurements (BAVN hereafter) for *any* number of qubits. We then proceed to explicitly provide *all* physically distinct BAVN proofs with up to 7 qubits.

A BAVN proof consists of an n -qubit quantum state and a set of single-qubit measurements that satisfy two requirements: (a) *Perfect correlations to define bipartite EPR's elements of reality*. Every single-qubit observable involved in the proof must satisfy EPR's criterion of elements of reality. (b) *Perfect correlations that contradict EPR's elements of reality*. The observables that satisfy EPR's condition *cannot* have predefined results, because it must be impossible to assign them values that satisfy all the perfect correlations predicted by quantum mechanics.

Perfect correlations are necessary to establish elements of reality and to prove that they are incompatible with quantum mechanics. Therefore, the states we are interested in must be simultaneous eigenstates of a sufficient number of commuting n -fold tensor products of single-qubit operators. Suppose that A and B are single-qubit

operators on the same qubit. If they are different, they cannot be commuting operators. The only way to make the n -fold tensor products be commuting operators is to choose A and B to be *anticommuting* operators. Therefore, in an AVN proof, all the local operators corresponding to the same qubit must be anticommuting operators. The maximum number of anticommuting single-qubit operators is 3. Therefore, without loss of generality, we can restrict our attention to a specific set of 3 single-qubit anticommuting operators on each qubit, e.g. the Pauli matrices $X = \sigma_x$, $Y = \sigma_y$, and $Z = \sigma_z$. This leads us to the notion of stabilizer states. An n -qubit *stabilizer state* is defined as the simultaneous eigenstate with eigenvalue 1 of a set of n independent (in the sense that none of them can be written as a product of the others) commuting elements of the Pauli group, defined as the group, under matrix multiplication, of all n -fold tensor products of X , Y , Z , and the identity $\mathbf{1}$. The n independent elements are called *stabilizer generators* and generate a maximally Abelian subgroup called the *stabilizer group* of the state [26]. The 2^n elements of the stabilizer group are called *stabilizing operators*, and provide all the perfect correlations of the stabilizer state.

Moreover, since any stabilizer state is local Clifford equivalent (i.e., equivalent under the local unitary operations that map the Pauli group to itself under conjugation) to a graph state [27], then we can restrict our attention to graph states. A *graph state* [28] is a stabilizer state whose generators can be written with the help of a graph. $|G\rangle$ is the n -qubit state associated to the graph G , which gives a recipe both for preparing $|G\rangle$ and for obtaining n stabilizer generators that uniquely determine $|G\rangle$. On one hand, G is a set of n vertices (each of them representing a qubit) connected by edges (each of them representing an Ising interaction between the connected qubits). On the other hand, the stabilizer generator g_i is obtained by looking at the vertex i of G and the set $N(i)$ of vertices which are connected to i , and is defined by

$$g_i = X_i \bigotimes_{j \in N(i)} Z_j, \quad (1)$$

where X_i , Y_i , and Z_i denote the Pauli matrices acting on the i th qubit. $|G\rangle$ is the unique n -qubit state that fulfills

$$g_i |G\rangle = |G\rangle, \text{ for } i = 1, \dots, n. \quad (2)$$

Therefore, the stabilizer group is

$$S(|G\rangle) = \{s_j, j = 1, \dots, 2^n\}; \quad s_j = \prod_{i \in I_j(G)} g_i, \quad (3)$$

where $I_j(G)$ denotes a subset of $\{g_i\}_{i=1}^N$. The stabilizing operators of $|G\rangle$ satisfy

$$s_j |G\rangle = |G\rangle. \quad (4)$$

Equations like (4) are the ones that can be used to establish elements of reality and prove their incompatibility with quantum mechanics.

Although graph states are now ubiquitous in quantum information theory due to their role as code words of quantum error correcting codes [26], or in measurement-based quantum computation [29], or due to their use in the classification of entanglement [30], the first $n > 2$ -qubit graph states were the GHZ states and appeared in the context of AVN proofs. It is then not that surprising that, when we want to obtain BAVN proofs, we go back to graph states. Indeed, DiVincenzo and Peres already showed that the requirement (b) does not only occur for GHZ states, but is also inherent to all standard code words of quantum error correcting codes [31]. More recently, Scarani *et al.* have shown that (b) holds for cluster states constructed on square lattices of any dimension [32]. Furthermore, a positive by-product of focusing on graph states is that graph states associated to connected graphs have been exhaustively classified. There is only one 2-qubit graph state (equivalent to a Bell state), only one 3-qubit graph state (the GHZ state), two 4-qubit graph states (the GHZ and the cluster state), four 5-qubit graph states, eleven 6-qubit graph states, and twenty-six 7-qubit graph states [28].

Therefore, our problem reduces to the following: If n qubits were distributed between 2 parties, which n -qubit graph states and possible distributions of qubits allow a bipartite AVN proof using only single-qubit observables?

Note that, even considering only up to 7 qubits, there are hundreds of states and possible distributions that could potentially lead to a BAVN proof. Remarkably, this is not the case.

Our starting point is the observation that requirement (b) is satisfied by *any* graph state.

Lemma 1.—Any graph state associated to a connected graph of 3 or more vertices leads to algebraic contradictions with the concept of elements of reality (when each qubit is distributed to a different party).

This result was anticipated in [30, 31, 32]. The interest of the following proof is that it provides methods for obtaining explicit examples of sets of perfect correlations satisfying (b).

Proof.—If qubit i is connected to qubit j , and j is connected to k , there are two possibilities. One is that i is not connected to k . Then, no theory exists that assigns predefined values -1 or 1 to Y_i , Z_i , X_j , Y_j , Y_k , and Z_k simultaneously satisfying the four equations

$$g_i g_j |G\rangle = |G\rangle, \quad (5a)$$

$$g_j |G\rangle = |G\rangle, \quad (5b)$$

$$g_j g_k |G\rangle = |G\rangle, \quad (5c)$$

$$g_i g_j g_k |G\rangle = |G\rangle, \quad (5d)$$

since $g_i g_j \cdot g_j \cdot g_j g_k$ (where “ \cdot ” means matrix multiplication) is equal, not to $g_i g_j g_k$ (as expected in any theory

with predefined values), but to $-g_i g_j g_k$.

The other possibility is that qubit i is also connected to k . Then, no theory exists that assigns predefined values -1 or 1 to X_i , Z_i , X_j , Z_j , X_k , and Z_k simultaneously satisfying the four equations

$$g_i |G\rangle = |G\rangle, \quad (6a)$$

$$g_j |G\rangle = |G\rangle, \quad (6b)$$

$$g_k |G\rangle = |G\rangle, \quad (6c)$$

$$g_i g_j g_k |G\rangle = |G\rangle, \quad (6d)$$

since $g_i \cdot g_j \cdot g_k$ is equal to $-g_i g_j g_k$. ■

Any set of equations associated to the stabilizing operators containing a subset satisfying (b) also satisfies (b). Therefore, given a graph state associated to a connected graph of $n > 3$ vertices, there are *thousands* of possible different subsets of equations satisfying (b). Most of them involve the three Pauli matrices of all the qubits, but some of them do not. However, in our BAVN proofs it is relevant that the three Pauli matrices of *each and every one* of Alice's (Bob's) qubits can be regarded as EPR elements of reality, because we are interested in new BAVN proofs involving new classes of graph states, not those which are mere consequences of previously considered graph states of fewer qubits.

Therefore, the problem we have to solve is that of finding out for which graph states and distributions are all the three Pauli matrices for all the single-qubit elements of reality in a bipartite scenario. A distribution of n qubits between Alice and Bob is said to permit *bipartite elements of reality* when, for each and every qubit, the results of measuring two Pauli matrices on Alice's (Bob's) qubit j can be predicted with certainty from the results of measurements on Bob's (Alice's) qubits only.

Let us define the *reduced stabilizer* of Alice's (Bob's) qubits as the one obtained by tracing out Bob's (Alice's) qubits. A necessary and sufficient condition for bipartite elements of reality is the following.

Lemma 2.—A distribution of n qubits between Alice (who is given n_A qubits) and Bob (who is given $n_B = n - n_A$ qubits) permits bipartite elements of reality if and only if $n_A = n_B$, and the reduced stabilizer of Alice's (Bob's) qubits contains *all* possible variations with repetition of the four elements, $\mathbb{1}$, X , Y , and Z , choose n_A (n_B), without repeating any of them.

Proof.—Suppose that two Pauli matrices of Alice's qubit 1, e.g. X_1 and Y_1 are elements of reality. Then each of them must be predicted with certainty from Bob's measurements. That is, the reduced stabilizer of Alice's qubits must contain

$$X_1 \otimes \mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_{n_A}, \quad (7a)$$

$$Y_1 \otimes \mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_{n_A}. \quad (7b)$$

Therefore, the third Pauli matrix of Alice's qubit 1 must also be an element of reality, since the product of (7a)

and (7b), which must belong to the reduced stabilizer of Alice's qubits, is

$$Z_1 \otimes \mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_{n_A}. \quad (8)$$

The same must happen with the three Pauli matrices of Alice's qubits $2, \dots, n_A$. Therefore, the reduced stabilizer of Alice's qubits must also contain

$$\mathbb{1}_1 \otimes X_2 \otimes \mathbb{1}_3 \otimes \dots \otimes \mathbb{1}_{n_A}, \quad (9a)$$

$$\mathbb{1}_1 \otimes Y_2 \otimes \mathbb{1}_3 \otimes \dots \otimes \mathbb{1}_{n_A}, \quad (9b)$$

$$\mathbb{1}_1 \otimes Z_2 \otimes \mathbb{1}_3 \otimes \dots \otimes \mathbb{1}_{n_A}, \dots, \quad (9c)$$

$$\mathbb{1}_1 \otimes \dots \otimes \mathbb{1}_{n_A-1} \otimes Z_{n_A}. \quad (9d)$$

Moreover, the reduced stabilizer of Alice's qubits must contain all the possible products of the Eqs. (7a)–(9d); that is, all possible variations with repetition of the four elements, $\mathbb{1}$, X , Y , and Z , choose n_A , which are $4^{n_A} = 2^{2n_A}$. Furthermore, a similar reasoning applies to the three Pauli matrices of each and every one of Bob's qubits. Therefore, the reduced stabilizer of Bob's qubits must also contain all the possible products of

$$X_{n_A+1} \otimes \mathbb{1}_{n_A+2} \otimes \dots \otimes \mathbb{1}_{n_B}, \dots, \quad (10a)$$

$$\mathbb{1}_{n_A+1} \otimes \dots \otimes \mathbb{1}_{n_B-1} \otimes Z_{n_B}. \quad (10b)$$

But the total stabilizer only has $2^{n_A+n_B}$ terms; therefore the only possibility is that $n_A = n_B$. In addition, note that there is no space for any of the variations with repetition to be repeated. ■

Most of the graph states *cannot* be used in BAVN proofs. The remarkable point is that there are a few graph states and distributions of qubits that satisfy the requirements of Lemma 2, and therefore simultaneously fulfill (a) and (b). Moreover, since Lemma 2 is a necessary and sufficient condition, when we apply it to every possible distribution of qubits of all possible graph states, we obtain a *complete* classification of all possible BAVN proofs.

With $n < 8$ qubits, and modulo single-qubit unitary transformations, the only states and distributions of qubits that allow BAVN proofs are the following. There is only one graph state with 4 qubits:

$$|\psi_{4a}\rangle = \frac{1}{2}(|00\rangle|\bar{0}\bar{0}\rangle + |01\rangle|\bar{0}\bar{1}\rangle + |10\rangle|\bar{1}\bar{0}\rangle - |11\rangle|\bar{1}\bar{1}\rangle), \quad (11)$$

where $|00\rangle|\bar{0}\bar{0}\rangle = |\sigma_z = 0\rangle_1 \otimes |\sigma_z = 0\rangle_2 \otimes |\sigma_x = 0\rangle_3 \otimes |\sigma_x = 0\rangle_4$, with qubits 1 and 2 in Alice's side, and qubits 3 and 4 in Bob's. The state $|\psi_{4a}\rangle$ corresponds to the graph state no. 4 according to Hein *et al.* [28], with its qubits distributed as in Fig. 1, distribution 4a. Note that any other non-equivalent distribution of qubits does not allow BAVN proofs (see Fig. 1). This BAVN proof is precisely the one introduced in [17]. The new result is that the proof in [17] is *the only one* with 4 qubits and single qubit measurements.

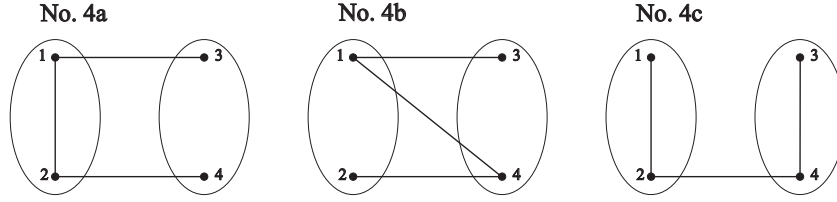


FIG. 1: Bipartite distributions of the 4-qubit cluster state (graph state no. 4 according to Hein *et al.* [28]). Distribution 4a permits bipartite elements of reality and BAVN proofs. Distribution 4b is physically equivalent (it is just relabeling the basis). Distribution 4c is not equivalent to the other two, and does not permit bipartite elements of reality.

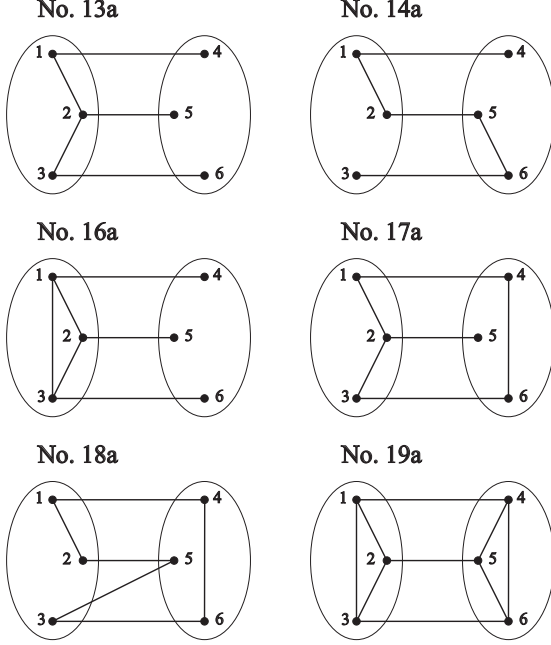


FIG. 2: Bipartite distributions of the 6-qubit graph states that permit bipartite elements of reality and BAVN proofs. The graphs' nomenclature follows Hein *et al.* [28], but the labeling of the qubits is different: Qubits 1, 2, and 3 belong to Alice, and qubits 4, 5, and 6 belong to Bob.

Between 5 and 7 qubits, there are only 6 possible states and distributions leading to BAVN proofs. All of them are 6-qubit states in which each party has 3 qubits. Their corresponding graphs are summarized in Fig. 2. The explicit expressions of each state can be obtained from its graph using (1) and (2). Two 6-qubit graph states have been recently prepared in the laboratory [21, 22], but none of them allows BAVN proofs. A 6-qubit BAVN proof constitutes an interesting experimental challenge for the near future.

This work was sparked by questions made by F. Verstraete and M. Żukowski. The authors thank H. Briegel, W. Dür, O. Gühne, A. J. López-Tarrida, and M. van den Nest for their useful comments, and acknowledge support by the Spanish MEC Project No. FIS2005-07689, and the Junta de Andalucía Excellence Project No. P06-

FQM-2243.

* Electronic address: adan@us.es

- [1] D.M. Greenberger, M.A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, Holland, 1989), p. 69.
- [2] N.D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990).
- [3] J.S. Bell, Physics (Long Island City, NY) **1**, 195 (1964).
- [4] M. Żukowski, Phys. Lett. A **157**, 198 (1991).
- [5] R.K. Clifton, M.L.G. Redhead, and J.N. Butterfield, Found. Phys. **21**, 149 (1991).
- [6] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).
- [7] M. Żukowski *et al.*, Acta Phys. Pol. A **93**, 187 (1998).
- [8] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
- [9] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
- [10] N.D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
- [11] A. Cabello, Phys. Rev. Lett. **86**, 1911 (2001).
- [12] A. Cabello, Phys. Rev. Lett. **87**, 010403 (2001).
- [13] Z.-B. Chen *et al.*, Phys. Rev. Lett. **90**, 160408 (2003).
- [14] C. Cinelli *et al.*, Phys. Rev. Lett. **95**, 240405 (2005).
- [15] T. Yang *et al.*, Phys. Rev. Lett. **95**, 240406 (2005).
- [16] A.I. Lvovsky, Phys. Rev. Lett. **88**, 098901 (2002).
- [17] A. Cabello, Phys. Rev. Lett. **95**, 210401 (2005).
- [18] A. Cabello, Phys. Rev. A **72**, 050101(R) (2005).
- [19] G. Vallone *et al.*, Phys. Rev. Lett. **98**, 180502 (2007).
- [20] J.T. Barreiro *et al.*, Phys. Rev. Lett. **95**, 260501 (2005).
- [21] Q. Zhang *et al.*, Nature Physics **2**, 678 (2006).
- [22] C.-Y. Lu *et al.*, Nature Physics **3**, 91 (2007).
- [23] A. Cabello, Phys. Rev. A **73**, 022302 (2006).
- [24] A. Cabello, Phys. Rev. Lett. **97**, 140406 (2006).
- [25] M. Barbieri *et al.*, Phys. Rev. Lett. **97**, 140407 (2006).
- [26] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
- [27] M. Van den Nest, J. Dehaene, and B. De Moor, Phys. Rev. A **69**, 022316 (2004).
- [28] M. Hein, J. Eisert, and H.J. Briegel, Phys. Rev. A **69**, 062311 (2004).
- [29] R. Raussendorf and H.J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
- [30] M. Hein *et al.*, in *Quantum Computers, Algorithms and Chaos*, edited by G. Casati *et al.* (IOS Press, Amsterdam, 2006).
- [31] D.P. DiVincenzo and A. Peres, Phys. Rev. A **55**, 4089 (1997).
- [32] V. Scarani *et al.*, Phys. Rev. A **71**, 042325 (2005).